© Smirnov O., Didyk O., Dreyev O., Smirnov S. GERT model complex for cloud antivirus security of telecommunication system // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 3, p. 251-262.

КОМПЛЕКС GERT-МОДЕЛЕЙ ТЕХНОЛОГИИ ОБЛАЧНОЙ АНТИВИРУСНОЙ ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ

Алексей Смирнов, Александр Дидык, Александр Дреев, Сергей Смирнов

Кировоградский национальный технический университет, Украина

СМИРНОВ Алексей Анатольевич, д.т.н.

Год и место рождения: 1977 год, г. Кировоград, Украина.
Образование: Харьковский военный университет, 1999 год.
Должность: заведующий кафедрой программирования и защиты информации с 2014 года.
Научные интересы: защита информации, телекоммуникации.
Публикации: более 250 научных публикаций, среди которых монографии, учебные пособия, научные статьи и патенты на изобретения.
E-mail: dr.SmirnovOA@gmail.com

ДИДЫК Александр Константинович, к.т.н.

Год и место рождения: 1979 год, г. Запорожье, Украина.
Образование: Кировоградский государственный технический университет, 2000 год.
Должность: доцент кафедры автоматизации производственных процессов с 2009 года.
Научные интересы: защита информации, телекоммуникации.
Публикации: более 30 научных публикаций, среди которых научные статьи, материалы и тезисы конференций..
E-mail: didyk_s@mail.ru

ДРЕЕВ Александр Николаевич, к.т.н.

Год и место рождения: 1976 г., г. Кировоград, Украина.
Образование: Кировоградский государственный педагогический университет им. В.Винниченко, 1999 год.
Должность: преподаватель кафедры программирования и защиты информации.
Научные интересы: сжатие информации, компьютерные сети, защита информации.
Публикации: более 30 научных публикаций, среди которых монографии, научные статьи, материалы и тезы докладов на конференциях.
E-mail: drey_sanya@ukr.net

СМИРНОВ Сергей Анатольевич

Год и место рождения: 1981 год, г. Кировоград, Украина
Образование: Кировоградский национальный технический университет 2009 год
Должность: аспирант с 2014 года.
Научные интересы: компьютерные сети, защита информации.
Публикации: 19 научных публикаций, среди которых научные статьи, материалы и тезисы докладов на конференциях.
E-mail: Smirnov.Ser.81@gmail.com

Аннотация. *В данной статье разработано комплекс математических GERT-моделей технологии облачной антивирусной защиты телекоммуникационной системы (ТКС), что позволило получить аналитические выражения для расчета времени передачи файлов метаданных и формирования и доставки команд передачи управления. Разработана математическая модель и проведено исследование вероятностно-временных характеристик алгоритмов и программ формирования и обработки метаданных в облачных антивирусных системах. Ее отличительной особенностью является учет необходимости формирования команд передачи*

управления программному клиенту ТКС. На втором этапе моделирования разработаны GERT-модели технологии формирования и обработки метаданных в облачных антивирусных системах. Особенностью данных моделей является учет ряда технологических особенностей ТКС (гетерогенность, многосвязность, возможность разбиения файла метаданных и команд передачи управления на кадры и др.).

Ключевые слова: *защита информации, облачные антивирусы, телекоммуникационные сети, GERT-модель.*

Вступление

Технологии облачной антивирусной защиты включают в себя сложные математические методы и программно-аппаратные комплексы хранения, обработки и передачи данных, компьютеризированные средства управления, телекоммуникаций и др. Постоянное развитие средств вычислительной техники и комплексов автоматизации, а также повышающийся спрос на услуги облачных антивирусных систем приводит к увеличению объемов передаваемых в данные системы метаданных.

В настоящее время прогресс в области облачных технологий, развитие вычислительных и телекоммуникационных технологий, а также появившееся научно-методическое обеспечение проектирования облачных антивирусных систем [1-6], создали реальную базу для повышения качества проектных работ, унификации средств антивирусной защиты данных и создания условий оптимизации процесса обработки метаданных в облачных антивирусных системах. Однако рост требований к точности моделирования и качеству технических разработок требует учета множества объективных и субъективных факторов, возникающих в процессе функционирования ТКС. Такими факторами являются:

– гетерогенность ТКС, содержащих различные компоненты многие из которых сами являются сложными, многофункциональными системами;

– многосвязность и крупномасштабность ТКС;

– децентрализация информационных и вычислительных ресурсов в глобальной сети;

– подверженность различного рода внешним и внутренним вторжениям (особенно вирусным атакам);

– наукоемкость и непрерывность развития, базирование на перспективных технических и программных разработках и др.

Анализ существующих исследований

Анализ литературы [13-27] показал, что в настоящее время существует множество подходов и направлений математического моделирования ТКС и компьютерных сетей. Однако большинство задач, возникающих при управлении, оптимизации, тестировании, оценке вероятностно-временных характеристик, параметров надежности, отказоустойчивости, информационной и функциональной безопасности значительно упрощаются, если их рассматривать на теоретико-графовых моделях.

В работах [28-31] проведен анализ и сравнительные исследования основных направлений графового подхода математического моделирования информационно-телекоммуникационных и компьютерных систем и сетей. При этом выявлено, что большинство из указанных выше задач сетевого планирования с минимальной погрешностью можно успешно решить с помощью математического моделирования на основе GERT-сетей.

Разработка графо-аналитических моделей GERT связана с именем американского математика Алана Прицкера [32, 33]. Однако потенциальные возможности математического аппарата GERT-сетей в отдельных направлениях и приложениях современных ТКС в настоящее время еще полностью не использованы.

В этой связи возникает проблема разработки математических моделей наиболее точно формализующих технологию функционирования ТКС. Особенно важной при этом является задача математического описания технологии облачной антивирусной защиты ТКС с учетом ряда основных факторов (гетерогенность, многосвязность и др.).

Основная часть исследования

Для решения поставленной задачи рассмотрим общую структуру технологии облачной антивирусной защиты ТКС.

Структура технологии облачной антивирусной защиты

Проведенные исследования процесса сбора, хранения и обработки метаданных в облачных антивирусных системах показал, что общую структуру технологии облачной антивирусной защиты можно представить в виде схемы рис. 1.

Рассмотрим более подробно предназначение каждого из блоков.

Поток данных из каналов связи поступает на телекоммуникационный адаптер (сетевое приложение), основная задача которого выделение из потока данных отдельных приложений и формирование файлов (команд передачи управления) для обработки в программном клиенте, а также беспрепятственная передача метаданных в канал связи телекоммуникационной сети.

Программный клиент – модуль, размещенный на компьютере-клиенте, предназначен для организации взаимодействия аппаратной и программной (приложения) составляющих системы, представления подозрительных файлов в формирователь метаданных, а также представления в удобном формате (построение таблиц, графиков, диаграмм и т.д.) результатов работы облачной антивирусной системы. Программный клиент функционально связан с анализатором файлов – пакетом программ, предназначенным для осуществления предварительного сигнатурного и эвристического анализа (сравнение с установленными эталонами,

проверка допустимости значений и т.д.) на клиентской части системы.

Формирователь метаданных предназначен для выделения специальных сигнатур подозрительных файлов с помощью современных средств хеширования файлов. Специальные сигнатуры через описанный выше адаптер передаются в канал связи телекоммуникационной сети. Передача в телекоммуникационной сети через промежуточные узлы коммутации (блок передачи метаданных) проходит в соответствии с известными протоколами и усовершенствованными методами управления информационным трафиком.

Анализатор метаданных в облачном антивирусе выявляет угрозы и проверяет качество принятых решений на ошибки, после чего ищет источники распространения угроз. Найденные источники также проходят автоматическую контрольную проверку – чтобы исключить ложные срабатывания. Полученная с помощью анализатора информация о только что появившихся угрозах и источниках их распространения оперативно заносится в архив злоумышленного программного обеспечения и становится доступной всем остальным пользователям продукта.

Информация о заражениях используются для самообучения анализатора метаданных, вследствие чего она быстро реагирует на новейшие разработки злоумышленников и в автоматическом режиме выявляет активные угрозы на компьютерах пользователей. Используемая для самообучения информация о заражениях включает, в том числе, вердикты, полученные с помощью сигнатурного и эвристического детектирования.

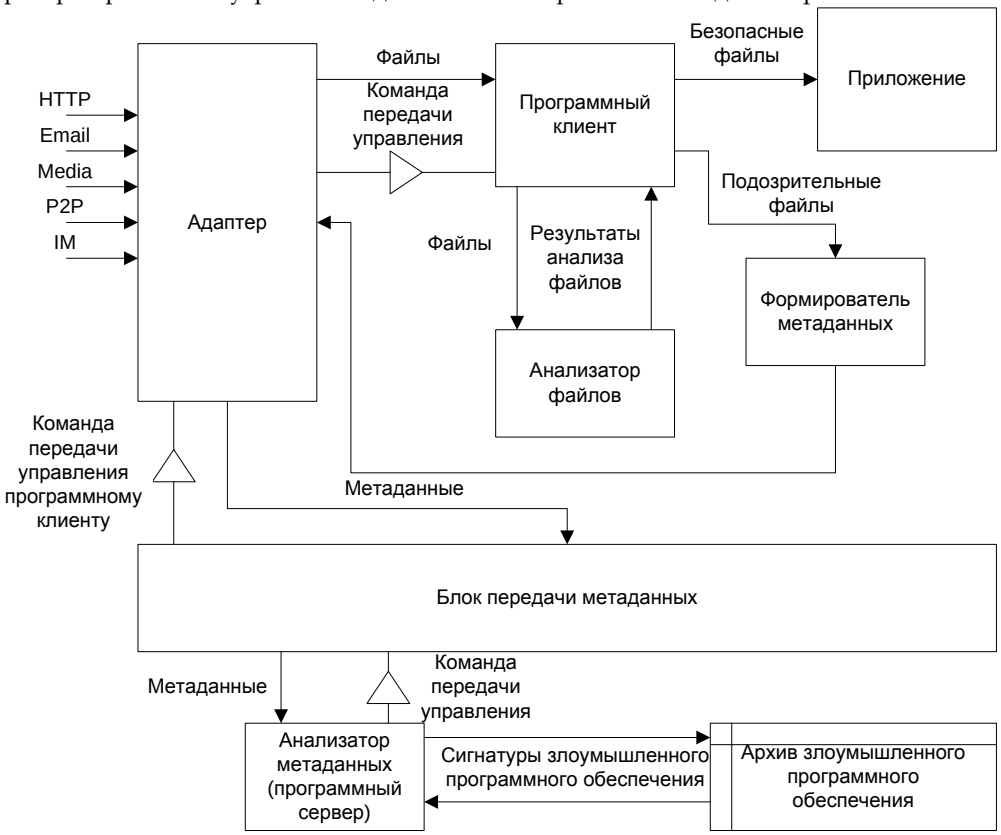


Рис. 1. Структурная схема технологии облачной антивирусной защиты

Собирая и обрабатывая данные о подозрительной активности от каждого участника сети, облачная защита представляет собой мощную экспертную систему, направленную на анализ киберкриминальной активности. Данные, необходимые для блокирования атаки, которой подвергся компьютер любого пользователя, передаются всем участникам облачной сети, что позволяет предотвращать последующие заражения.

Проведенные исследования показали, что для реализации многопользовательских распределенных приложений (каковой является и облачная антивирусная система) должен быть предусмотрен интерфейс сокетов.

Сокеты (*sockets* – «гнезда») – это один из способов передачи данных и обмена информацией между компьютерами. Сокеты являются программными конечными точками сетевого соединения. Для работы с сокетами необходимо использовать некоторый протокол на основе TCP/IP и программный порт транспортного уровня Windows. Сокеты делятся на три основных типа [2].

Клиентские сокеты инициализируют соединение со стороны клиента с серверным сокетом на удаленной машине. Для того чтобы открыть соединение, клиентский сокет должен «знать» *IP*-адрес удаленной машины и номер порта, используемого серверным сокетом. Клиент посылает серверу запрос на соединение. Серверные сокеты сами не занимаются установлением связи с клиентскими сокетами. Эту задачу выполняют слушающие сокеты, встроенные в серверные сокеты.

Запрос на подключение нового клиента получает слушающий сокет, который ставит его в очередь. После того, как серверный сокет освободится от текущей работы, он обрабатывает запрос из очереди и создает слушающий сокет для нового соединения. Серверные сокеты устанавливают соединение с клиентским сокетом в ответ на его запрос. Клиентский сокет получает описание серверного сокета, после чего соединение считается установленным [2].

Проведем математическую формализацию технологии передачи и обработки метаданных в облачных антивирусных системах и определим основные временные характеристики этих процессов.

Оценка времени обработки метаданных в анализаторе облачных антивирусных систем

Время обработки метаданных в анализаторе облачных антивирусных систем (программным сервером) определим путем нахождения суммы случайного числа независимых случайных величин $\xi_1, \xi_2, \ldots$ с одним и тем же распределением F и производящей функцией моментов $M(s)$. Пусть N – целочисленная случайная величина с производящей функцией $A(s) = \sum P_i s^i$ и не зависящая от всех ξ_j. Тогда случайная сумма $\xi_1 + \ldots + \xi_N$ имеет распределение, описываемое производящей функцией моментов

$$\chi(s) = W(M(s)), \quad (1)$$

где $W(s)$ – производящая функция, описывающая случайное число запрашиваемых программным клиентом элементов метаданных, $M(s)$ – производящая функция моментов, характеризующая случайное время обработки одного элемента метаданных.

Рассмотрим метод расчета времени обработки при описании числа затребованных программным клиентом элементов метаданных равномерным распределением с целочисленными значениями. Число параметров в задании может изменяться от h до λ. Производящая функция моментов этого распределения с учетом того, что все события считаются равновероятными со значением $\overline{p}$, равна

$$M(s) = \overline{p}\left(e^{hs} + e^{(h+1)s} + \ldots + e^{(\ell-1)s} + e^{\ell s}\right) = \left(\overline{p}\left(e^{hs} - e^{(\ell+1)s}\right)\right) \Big/ \left(1 - e^{s}\right).$$

Производящая функция этого распределения $W(s) = \left(\overline{p}\left(s^h - s^{(\ell+1)}\right)\right) \Big/ (1-s)$. Для оценки случайного времени обработки одного элемента метаданных используем равномерное непрерывное распределение с параметрами a и b. Тогда в соответствии с (1) $\chi(s)$ можно вычислить как

$$\chi(s) = \overline{p}\left(\frac{\left(\frac{e^{as} - e^{bs}}{(a-b)s}\right)^h - \left(\frac{e^{as} - e^{bs}}{(a-b)s}\right)^{\ell+1}}{1 - \frac{e^{as} - e^{bs}}{(a-b)s}}\right). \quad (2)$$

Дифференцируя $\chi(s)$ по переменной s и приравнивая в полученных выражениях величину s нулю, получаем первый μ_1 и второй μ_2 моменты относительно начала координат и, соответственно, среднее значение t_s и дисперсию D времени обработки одного элемента метаданных, переданных по запросу программного клиента

$$\mu_1 = t_{cp}^{(o)} = \left.\frac{\partial(\chi(s))}{\partial s}\right|_{s=0} = \frac{(h+\ell)(a+b)}{4}, \quad (3)$$

$$J^{(o)} = \mu_2 - \mu_1^2 = \left.\frac{\partial^2(\chi(s))}{\partial s^2}\right|_{s=0} - \left(\left.\frac{\partial(\chi(s))}{\partial s}\right|_{s=0}\right)^2 = \frac{(h+\ell)(b-a)^2}{24}. \quad (4)$$

В случае, когда анализатор метаданных выполняет обработку файлов различных, независимых информационных потоков, число требований программного клиента на формирование, анализ и обработку управляющих команд может быть описано распределением Пуассона [7].

В этом случае производящая функция распределения Пуассона равна

$$W(s) = e^{\lambda s - \lambda}.$$

Отсюда производящая функция моментов времени формирования управляющих команд и выполнения задания программы-клиента равна

$$\chi(s) = e^{\left(-\lambda + \lambda \frac{e^{as} - e^{bs}}{(a-b)s}\right)}. \quad (5)$$

Из выражения (5) находим среднее время выполнения задания формирования управляющей команды и его дисперсию

$$t_{cp}^{(\phi)} = \frac{\lambda(a+b)}{2}, \quad (7)$$

$$J^{(\phi)} = \frac{\lambda(a^2 + ab + b^2)}{3}. \quad (8)$$

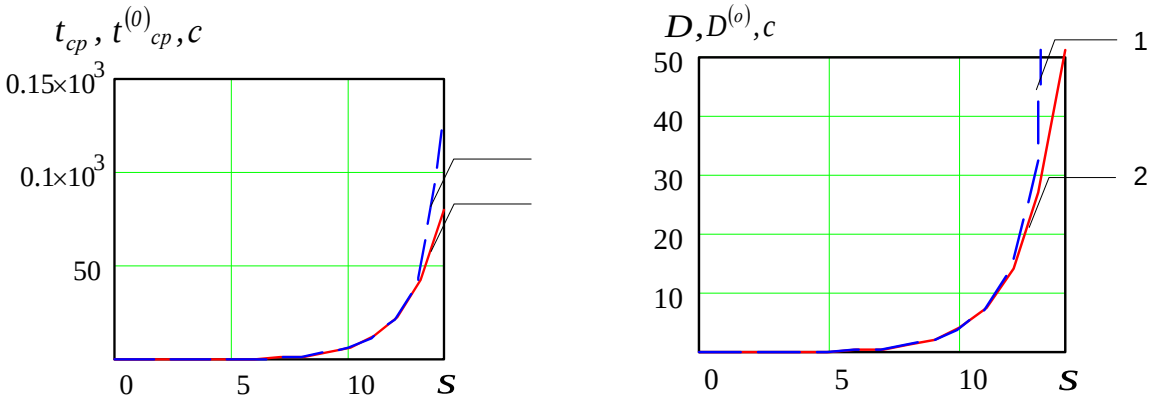
Проведем анализ взаимовлияния приведенных в 2, 4 и 7, 8 временных характеристик на общее время обработки метаданных и формирования управляющих команд.

На рис. 2 представлены графики общего времени $t_{cp}(s)$ (график 1) и времени обработки метаданных $t_{cp}^{(o)}(s)$ (график 2) а также графики джиттера $D(s)$ общего времени (график 1) и времени обработки метаданных $D^{(o)}(s)$ (график 2) в условиях когда $a = 0,4$; $b = 0,7$; $h = 0,3$; $\ell = 1$; $\overline{p} = 0,3$; $\lambda = 1200$.

Из графиков видно, что учет временных характеристик формирования управляющих сигналов позволит повысить точность результатов

оценки временных характеристик до 1,7 раз, и характеристик джиттера до 4,5 раз.

Таким образом, разработана и исследована математическая модель ТКС, позволяющая оценить временные характеристики обработки одного элемента метаданных и выработки управляющей команды. Ее отличительной особенностью является учет необходимости формирования команд передачи управления программному клиенту ТКС, что в целом повысило точность результатов математического моделирования в рассматриваемых условиях.



а) *б)*

Рис. 2. Графики $t_{cp}(s)$ и $t_{cp}^{(o)}(s)$ (а), $D(s)$ и $D^{(o)}(s)$ (б)

В большинстве случаев плотность распределения вероятностей времени обработки одного элемента метаданных и выработки управляющей команды имеет одну моду. Формулы (2), (7) можно использовать для предварительной оценки величины разброса распределения на основе правила «трех сигм». В то же время необходимость учета факторов, приведенных ранее требует разработки более сложных моделей.

Для решения данной задачи используем графовый подход *GERT*-структур. В качестве аргументов целесообразности такого подхода и адекватности получаемых результатов математического моделирования приводят протестированные методы построения *GERT*-сетей, а для сложных технических систем проверенные методики предварительной регуляризации сложных *GERT*-структур. Приведенные в работах [3, 8-12] результаты моделирования говорят о повышении точности получаемых результатов до 10-15%.

В условиях рассматриваемого примера, использование средств *GERT*-моделирования позволяет оптимизировать структуру системы создания, передачи и обработки метаданных, а также формирования команд передачи управления, оценить производительность и возможности ее масштабирования при увеличении объема и сложности решаемых задач.

Поэтому для нахождения плотности распределения вероятностей времени обработки метаданных и выработки управляющих команд $\phi(x)$ далее будут использованы *GERT*-модели.

Разработка моделей телекоммуникационной системы формирования и обработки метаданных в облачных антивирусных системах

Разработка и использование современной высокопроизводительной микропроцессорной техники, развитие алгоритмов управления информационными потоками в ТКС, повышенный спрос на облачные технологии в совокупности с большими рисками, связанными с возможностью заражения компьютерными вирусами предопределяют постоянное увеличение интенсивности передачи метаданных в облачные антивирусные системы. При этом возникают сложности связанные с тем, что производительность и надежность каналов телекоммуникационных сетей достаточно сложно повысить, оставаясь в рамках схемы одного физического канала. Для этого надо менять протокол, а, возможно, и физический носитель канала, например, переходить на оптоволокно с заменой портов коммуникационных устройств.

Повысить производительность и надежность канала можно за счет применения избыточных физических связей. Одним из используемых на практике способов является использование механизма агрегирования связей. Все избыточные связи рассматриваются в качестве активных, и используются для повышения, как надежности (в случае дублирования данных), так и производительности за счет распределения нагрузки между каналами (примером может быть случай многопутевой маршрутизации в ТКС). Агрегированные каналы (в дальнейшем маршруты) или транки используются чаще всего в сетях *Fast Ethernet* и *Gigabit Ethernet* для повышения производительности магистральных связей [1-6]. Коммутаторы *Ethernet* используют технику транкинга для создания скоростных магистральных связей между коммутаторами, а также для повышения скорости сетевой работы серверов. В общем случае используются механизмы агрегирования, позволяющие объединить в один логический канал, связи различных скоростей, протоколов и устройств.

Анализ известных подходов математического моделирования показал, что в настоящее время актуальной задачей является разработка математических моделей и методов расчета вероятностно-временных характеристик телекоммуникационных трактов, состоящих из множества агрегированных маршрутов, соединяющих коммутаторы сети (многопутевой маршрутизации). Связано это во многом с тем, что современные узлы связи (маршрутизаторы ТКС) могут быть как безинерционными, так и вносящими существенные задержки при обработке кадров (пакетов) метаданных. В то же время следует учитывать, что алгоритмы управления должны гарантировать заданные показатели качества: среднюю скорость передачи *CIR. (Committed Information Rate)*; количество отклонений джиттера K_J, соответствующих средней скорости *CIR* и периоду контроля Π. Отметим, что допустимое превышение количества отклонений джиттера:

$$K_{J\,доп} = CIR \cdot \Pi . \qquad (9)$$

Разработаем модели агрегированных маршрутов в ТКС при передаче метаданных в облачные антивирусные системы при следующих условиях:

– локальная ТКС имеет такое быстродействие, что временем передачи пакетов в ее разделяемых сегментах можно пренебречь;

– модель маршрута отражает время передачи пакетов метаданных как непосредственно в агрегированном маршруте, так и во входных и выходных очередях узлов связи;

– модель учитывает время формирования команд передачи управления в соответствующем анализаторе (программном сервере).

Формирование множества маршрутов $\aleph_{баз}$ для каждого узла i представляет собой итерационный процесс, который создает предпосылку минимизации времени передачи метаданных и команд передачи управления программному клиенту.

Однако, несмотря на достоинства (использование множества путей передачи информации, пропорциональное распределение потока информации по каналам связи) такого подхода маршрутизации существует и ряд его недостатков, в частности, отсутствие учета вероятности искажения информации на базовом множестве маршрутов, растущей с увеличением $\left|\aleph_{баз}\right|$, и структурных особенностей выбранных маршрутов. Для устранения указанных недостатков необходимо найти оптимальное множество маршрутов передачи метаданных и команд передачи управления (оптимальную топологию подсети) в ТКС.

Пусть для канала $c \in \Im$ маршрута $s \in \aleph_{баз}$ вероятность искажения одного бита равна $q_s^{(c)}$, то есть вероятность «неискажения» бита равна $p_s^{(c)} = 1 - q_s^{(c)}$. Тогда для пуассоновского потока информации интенсивностью $\lambda \cdot \phi_s$ с пакетом длиной λ_p, проходящего в с-м канале связи s-го маршрута за время Δt, вероятность «неискажения» информации равна

$$p_s^{(c)}(\Delta t) = (1 - q_s^{(c)})^{\lambda \phi_s \ell_p \Delta t} . \qquad (10)$$

Соответственно вероятность $p_s(\Delta t)$ «неискажения» информации при передаче ее по *s*-му маршруту за время Δt равна

$$p_s(\Delta t) = \prod_{c \in \eta_s} (1 - q_s^{(c)})^{\lambda \phi_s \ell_p \Delta t} , \qquad (11)$$

то есть при передаче информационного потока интенсивностью λ с использованием многопутевой маршрутизации на базовом множестве $\aleph_{баз}$ маршрутов вероятность $p(\aleph_{баз}, \Delta t)$ «неискажения» равна

$$p(\aleph_{баз}, \Delta t) = \prod_{s \in \aleph_{баз}} \prod_{c \in \eta_s} (1\text{-}q_s^{(c)})^{\lambda \phi_s \ell_p \Delta t} \qquad (12)$$

и, соответственно, вероятность $q(\aleph_{баз}, \Delta t)$ искажения при тех же условиях

$$q(\aleph_{баз}, \Delta t) = 1 - \prod_{s \in \aleph_{баз}} \prod_{c \in \eta_s} (1\text{-}q_s^{(c)})^{\lambda \phi_s \ell_p \Delta t} . \qquad (13)$$

Анализ протоколов транспортного уровня *NGN*-сетей показал целесообразность организации передачи метаданных в облачные антивирусные системы и команд управления программным клиентам с квитированием.

Исследования известных алгоритмов передачи данных показали, что в настоящее время существует три основные способа обработки ответов на положительные и отрицательные подтверждения:

– стартстопный, или передача с остановкой и ожиданием (*SAW – Stop And Wait*), часто называемый блочным методом передачи;

– с возвращением на N кадров (*GBN – Go Back N*), также называемый потоковым методом передачи;

– метод выборочного (селективного) повтора (*SR – Selective Repeat*).

Исходя из логики формирования, передачи и обработки метаданных для решения поставленной задачи облачной антивирусной защиты ТКС представляется целесообразным использование алгоритма *SAW*.

Разработаем математическую модель для определения вероятностно-временных характеристик агрегированного маршрута и агрегированного соединения состоящего из нескольких последовательно соединенных каналов, для алгоритма передачи информационных пакетов *SAW*.

Расчет характеристик маршрута при параллельной работе без ограничения общности можно провести для случая передачи файла достаточно большой длины λ. Передаваемый файл делится на некоторое целое число m информационных пакетов равной длины.

Каждый из R маршрутов передачи данных передает некоторое количество информационных пакетов с суммарными объемами $\lambda_1, \lambda_2, ..., \lambda_R, \quad \lambda = \sum_{a=1}^{R} \lambda_a, \forall \lambda_a > n$. Информационные пакеты помещаются в выходных буферах передающего устройства и посылаются по

множеству маршрутов передачи данных. После поступления всех информационных пакетов во входные очереди приемного устройства производится сборка файла. Предполагается, что задержки на разборку и сборку информационного пакета пренебрежимо малы, по сравнению со временем его передачи по маршруту (каналу связи).

Время передачи одного информационного пакета по маршруту a характеризуется экспоненциальным распределением с параметром λ_a. Вероятность передачи информационного пакета через канал связи без искажений равна p_a.

Математическая модель технологии передачи метаданных и команд передачи управления по агрегированному маршруту в соответствии с алгоритмом *SAW*

Проведенные исследования показали, что в соответствии с протоколом обмена данными, в основу которого заложен алгоритм *SAW*, если кадр информационного пакета метаданных передан без искажений, то на передающую сторону посылается положительная квитанция (*ACK*) и начинается передача следующего кадра. Если кадр передан неверно, то на передающую сторону посылается отрицательная квитанция (*NACK*).

При поступлении отрицательной квитанции кадр передается повторно до тех пор, пока не будет передан без искажений. Число повторных передач по маршрутам ограничено, но его можно принять бесконечно большим, так как для реальных каналов вероятность $1-p_a$ обычно мала и при увеличении числа допустимых повторных передач β величина $(1-p_a)^{\beta}$ быстро стремится к 0. Тогда производящая функция моментов времени передачи кадра равна $M_a(s)=\lambda_a p_a / (\lambda_a p_a - s)$.

По маршруту a передается m_a кадров, поэтому производящая функция моментов времени его передачи по маршруту $M_{Ea}(s)$ будет иметь вид

$$M_{Ea}(s)=M^{m_a}(s)=\lambda_a^{m_a} p_a^{m_a} / (\lambda_a p_a - s)^{m_a}. \quad (14)$$

Выражение (12) определяет производящую функцию моментов распределения Эрланга порядка m_a с параметром $\lambda_a p_a$, плотностью:

$$\phi_a(x)=\lambda_a^{m_a} p_a^{m_a} x^{m_a-1} e^{(-\lambda_a p_a x)/(m_a-1)!} \quad (15)$$

и функцией распределения:

$$F_a(x)=1-e^{-\lambda_a p_a x}\sum_{i=0}^{m_a-1}\frac{1}{(m_a-1-i)!}(\lambda_a p_a x)^{m_a-1-i}. \quad (16)$$

Для нахождения времени передачи метаданных в облачные антивирусные системы и команд управления программным клиентам по агрегированному маршруту воспользуемся следующими допущениями.

Если случайные величины $\zeta_1,\ldots,\zeta_n$ независимы, то функция распределения $F(y)$ времени передачи метаданных и команд управления по маршруту, состоящему из R логических каналов определяется как произведение функций распределения отдельных каналов

$$F(y)=\prod_{a=1}^{R}F_a(y). \quad (17)$$

Функция распределения времени передачи метаданных и команд управления для канала a, $a\in\overline{1,R}$ по алгоритму *SAW*

$$F_a(x)=1-e^{-\lambda_a p_a x}\sum_{i=1}^{m_a-1}\frac{(\lambda_a p_a x)^{m_a-1-i}}{(m_a-1-i)!}.$$

Отсюда

$$F(y)=\prod_{a=1}^{R}\left(1-e^{-\lambda_a p_a x}\sum_{i=1}^{m_a-1}\frac{(\lambda_a p_a x)^{m_a-1-i}}{(m_a-1-i)!}\right).$$

Зная плотность распределения времени передачи метаданных и команд управления по маршруту $f(y)$, найдем его математическое ожидание и дисперсию из выражений:

$$t_c^{(a)}=M(y)=\int_{-\infty}^{\infty}yf(y)dy,\ \sigma_a^2=D(y)=\int_{-\infty}^{\infty}\left(y-t_c^{(a)}\right)^2 f(y)dy.$$

GERT*-модель технологии передачи метаданных и команд передачи управления по агрегированному маршруту в соответствии с алгоритмом *SAW

Проиллюстрируем *GERT*-модель одного маршрута при использовании стартстопного метода передачи *SAW*. На рис. 3. представлена стохастическая *GERT*-модель одного маршрута в режиме стартстопной передачи метаданных в облачные антивирусные системы

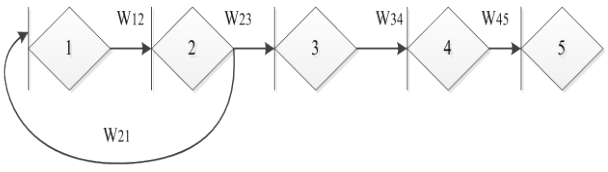


Рис. 3. Стохастическая *GERT*-модель одного маршрута в режиме стартстопной передачи метаданных

Дуга W_{12} отражает процесс передачи информационного пакета от формирователя к анализатору метаданных (см. рис. 1) где на транспортном уровне выполняется анализ правильности передачи информационного пакета и формирователю отправляется либо квитанция с подтверждением правильности передачи (дуга W_{23}, вероятность исполнения $1-p$), либо ей отправляется отрицательная квитанция (дуга W_{21} с вероятностью p).

Дуга W_{34} отражает процесс формирования команд передачи управления программному клиенту ТКС. Дуга W_{45} отражает процесс доставки команд передачи управления.

Пусть размер сообщения метаданных n, подвергаемого антивирусному анализу равен размеру информационного пакета метаданных, передаваемого по маршруту. Тогда производящие функции моментов времени передачи

информационного пакета метаданных $M_{12}(s)$ времени передачи положительной $M_{23}(s)$ и отрицательной квитанции $M_{21}(s)$, формирования команд передачи управления программному клиенту ТКС $M_{34}(s)$ равны соответственно:

$$M_{12}(s) = e^{sT_{12}},$$
$$M_{23}(s) = e^{sT_{23}},$$
$$M_{21}(s) = e^{sT_{21}},$$
$$M_{34}(s) = e^{sT_{34}},$$
$$M_{45}(s) = e^{sT_{45}},$$

где $T_{12} = n/\upsilon_1$ – время передачи информационного пакета метаданных; $T_{23} = T_{21} = n_1/\upsilon_1$ – время передачи квитанции в соответствии с протоколом транспортного уровня; $T_{34} = n/\upsilon_2$ – время формирования команд передачи управления программному клиенту ТКС; $T_{45} = T_{12} = n/\upsilon_1$ – время доставки команды передачи управления программному клиенту, n – длина передаваемого по маршруту информационного пакета; n_1 – длина передаваемой по обратному маршруту квитанции; υ_1 – теоретическая скорость передачи информационного пакета метаданных; υ_2 – теоретическая скорость формирования команд передачи управления программному клиенту.

В этом случае характеристики ветвей и параметры распределения можно представить в виде табл. 1.

В соответствии с алгоритмами определения эквивалентных W-функций $W_E(s)$, описанными в работах [3, 8-12], найдем эквивалентную W-функцию $W_E(s)$ стохастической модели для одного маршрута передачи метаданных:

$$W_E(s) = \frac{W_{12}W_{23}W_{34}W_{45}}{1 - W_{12}W_{21}} = \frac{(1-p)2e^{sT_{12}}e^{sT_{23}}e^{sT_{34}}}{1 - pe^{sT_{12}}e^{sT_{21}}} = \frac{qe^{sT_э^{(1)}}}{1 - pe^{sT_э^{(2)}}}, \quad (18)$$

где $q = 1 - p$; $T_э^{(1)} = \frac{\upsilon_2(2n + n_1) + \upsilon_1 n}{\upsilon_1\upsilon_2}$; $T_э^{(2)} = \frac{n + n_1}{\upsilon_1}$.

Таблица 1

Характеристики ветвей *GERT*-модели технологии передачи и обработки информационных пакетов метаданных по агрегированному маршруту в соответствии с алгоритмом *SAW*

№ п/п	Ветвь	*W*-функция	Вероятность	Производящая функция моментов
1.	*(1,2)*	W_{12}	*1*	$e^{sT_{12}}$
	(2,1)	W_{21}	*p*	$e^{sT_{21}}$
	(2,2)	W_{22}	*1-p*	$e^{sT_{23}}$
4.	*(2,4)*	W_{24}	*1*	$e^{sT_{34}}$
5.	*(4,5)*	W_{45}	*1*	$e^{sT_{12}}$

Выполняя деление числителя на знаменатель, получаем:

$$W_E(s) = qe^{sT_э^{(3)}} + qpe^{2sT_э^{(3)}} + qp^2e^{3sT_э^{(3)}} + ..., \quad (19)$$

где $T_э^{(3)} = \frac{(\upsilon_2 + \upsilon_1)n}{\upsilon_1\upsilon_2}$.

Выражение 15 описывает дискретное распределение с вероятностями qp^i в точках $T_э^{(3)}$, $2T_э^{(3)}$, $3T_э^{(3)}$... .

Для нахождения среднего времени передачи (формирования) метаданных и команд передачи управления по одному маршруту и его дисперсии σ^2 определим выражения для первого μ_1 и второго μ_2 моментов $W_E(s)$ относительно начала координат.

$$t_c = \mu_1 = \left.\frac{\partial W_E(s)}{\partial s}\right|_{s=0} = qT_э^{(3)}(1 + 2p + 3p^2 + 4p^3 + ...) =$$

$$= qT_э^{(3)} \cdot \frac{\partial}{\partial p}(1 + p + p^2 + p^3 + ... - 1) = qT_э^{(3)} \cdot \frac{\partial}{\partial p}\left(\frac{1}{1-p} - 1\right) = \frac{T_э^{(3)}}{q},$$

$$\mu_2 = \left.\frac{\partial^2 W_E(s)}{\partial s^2}\right|_{s=0} = \frac{T_э^{(3)2}}{q^2}(1 + 2p), \quad \sigma^2 = \mu_2 - \mu_1^2 = \frac{2T_э^{(3)2}}{q^2}p^2.$$

Однако, как было указано выше гетерогенность и многосвязность современных ТКС требует учета возможности использования агрегированных маршрутов при математическом моделировании. Поэтому найдем аналитические выражения для оценки случайного времени передачи метаданных в облачные антивирусные системы и команд передачи управления по агрегированному маршруту.

Эквивалентную W-функцию i-го маршрута можно представить как выражение:

$$W_E^{(i)}(s) = p_1^{(i)}e^{sT_{э1}^{(i)}} + p_2^{(i)}e^{sT_{э2}^{(i)}} + p_3^{(i)}e^{sT_{э3}^{(i)}} + \dots,$$

где $T_{э1}^{(i)}, T_{э2}^{(i)}, T_{э3}^{(i)}$ ... – моменты времени окончания передачи, формирования, а также доставки команд передачи управления программному клиенту ТКС; $p_1^{(i)}$, $p_2^{(i)}$, $p_3^{(i)}$ ... – вероятности этих событий.

Алгоритм нахождения плотности распределения времени, необходимого на передачу метаданных, а также формирование и доставку команд управления программному клиенту по агрегированному маршруту является итерационным.

На первом шаге алгоритма находим плотность вероятности времени передачи метаданных наиболее медленного их первых двух по

порядку маршрутов. Полученная плотность характеризует новую случайную величину, которая вместе со случайным временем передачи по третьему по порядку маршруту опять образует пару величин, для которых ищется плотность распределения максимальной из двух случайных величин и т.д.

Рассмотрим W-функции $W_E^{(1)}(s)$, $W_E^{(2)}(s)$ пары случайных величин, характеризующих время передачи метаданных и команд передачи управления по первому и второму маршрутам соответственно

$$W_E^{(1)}(s) = p_1^{(1)} e^{sT_{y1}^{(1)}} + p_2^{(1)} e^{sT_{y2}^{(1)}} + p_3^{(1)} e^{sT_{y3}^{(1)}} + \ldots + p_m^{(1)} e^{sT_{ym}^{(1)}},$$

$$W_E^{(2)}(s) = p_1^{(2)} e^{sT_{y1}^{(2)}} + p_2^{(2)} e^{sT_{y2}^{(2)}} + p_3^{(2)} e^{sT_{y3}^{(2)}} + \ldots + p_k^{(2)} e^{sT_{yk}^{(2)}}.$$

Пусть p_i и p_j вероятности дискретных распределений, характеризующих время передачи метаданных и команд передачи управления по первому и второму маршруту соответственно. Тогда для $\forall\left(i=\overline{1,m}\right)$; $\left(j=\overline{1,k}\right)$ находим $p_y = p_i p_j$, $y = \max\{i, j\}$, где p_y – вероятность дискретного распределения максимальной из двух случайных величин.

Так как алгоритм итерационный, то вероятности p_y в общем случае задают распределение нескольких случайных величин. Если маршрут y не последний, то добавляется маршрут $y+1$, и снова находится распределение максимальной из нескольких случайных величин и т.д. Процедуры повторяются до тех пор, пока не будет учтено влияние на общее время передачи метаданных и команд передачи управления всех составляющих маршрутов.

В этом случае эквивалентная W-функция времени передачи метаданных в облачные антивирусные системы, формирования и доставки команд передачи управления программному клиенту по агрегированному маршруту равна

$$W_E^{(a)}(s) = p_1 e^{sT_{y1}} + p_2 e^{sT_{y2}} + p_3 e^{sT_{y3}} + \ldots + p_\beta e^{sT_{y\beta}}, \quad (20)$$

где β – число значений распределения.

Среднее время и дисперсия времени передачи метаданных, формирования и доставки команд передачи управления находятся в соответствии с выражениями:

$$t_c^{(a)} = \left.\frac{\partial W_E(s)}{\partial s}\right|_{s=0} = \sum_{i=1}^{\gamma} p_i T_i,$$

$$\sigma^{(a)2} = \left.\frac{\partial^2 W_E(s)}{\partial s^2}\right|_{s=0} - \left(\left.\frac{\partial W_E(s)}{\partial s}\right|_{s=0}\right)^2 = \sum_{i=1}^{\gamma} p_i T_i^2 - \sum_{i=1}^{\gamma} p_i T_i,$$

где T_i – значения распределения; p_i – вероятности событий; γ – число логических каналов.

Если $\overline{W_E^{(a)}}(s)$ – эквивалентная W-функция цепочки последовательных каналов на маршруте, то

$$\overline{W_E^{(a)}}(s) = \prod_{i=1}^{Y} W_{E_Y}{}^{(a)}(s), \quad (21)$$

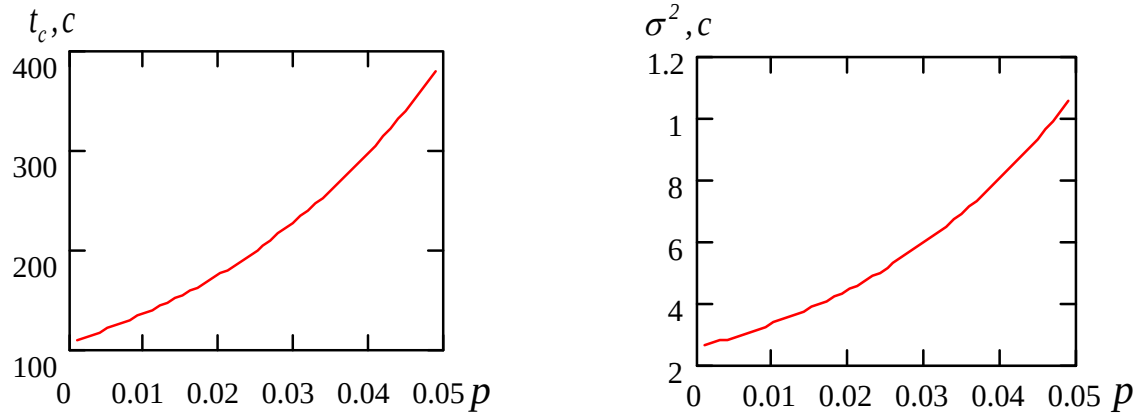
где Y – число последовательно проходимых сообщением метаданных и команды передачи управления агрегированных каналов. Плотность распределения времени прохождения этой последовательности каналов, очевидно, представляет собой дискретное распределение. Значения вероятностей находятся путем умножения рядов, каждый из которых определяется одним из выражений типа (20).

Найдем первую и вторую производные эквивалентная W-функция времени передачи метаданных в облачные антивирусные системы, формирования и доставки команд передачи управления программному клиенту по агрегированному маршруту и проведем исследования зависимости временных характеристик от вероятности передачи отрицательной квитанции о доставке информационных пакетов при условиях когда: вероятности передачи положительной и отрицательной квитанций вычисляются в соответствии с выражениями 10-12, $\upsilon_2 = 56$ *Гфлопс*, $\upsilon_1 = 10$*Мб / с*, 12*Мб / с*, …, 20*Мб / с*, $\beta = 1, 2, ..., 5$.

На рис. 4 представлены графики зависимости среднего времени и дисперсии передачи метаданных и формирования и доставки команд передачи управления от вероятности передачи отрицательной квитанции о доставке информационных пакетов.

Как видно из рисунков рост вероятности передачи отрицательной квитанции о доставке информационных пакетов приводит к значительному (до 4 раз) увеличению времени t_c. Это подтверждает необходимость использования дополнительных механизмов защиты и улучшения качества каналов связи на маршрутах.

В рассмотренной модели в качестве допущения было определено, что длина сообщения метаданных не превышает размера информационного пакета, определенного технологией передачи данных. Однако на практике гетерогенность технологий канального уровня подразумевает возможные изменения размеров информационных пакетов на пути следования по маршруту. Этот фактор целесообразно учесть и при разработке *GERT*-модели технологии передачи метаданных и команд передачи управления по агрегированному маршруту. Для решения этой задачи разработаем *GERT*-модель технологии передачи и обработки хеш-файла метаданных



а) *б)*

Рис. 4. Графики зависимости: а) t_c от вероятности p; б) σ^2 от вероятности p

Таким образом, разработана математическая *GERT*-модель технологии передачи метаданных и команд передачи управления по агрегированному маршруту в соответствии с алгоритмом *SAW*, которая отличается от известных учетом многосвязности (многопутевой маршрутизации) ТКС.

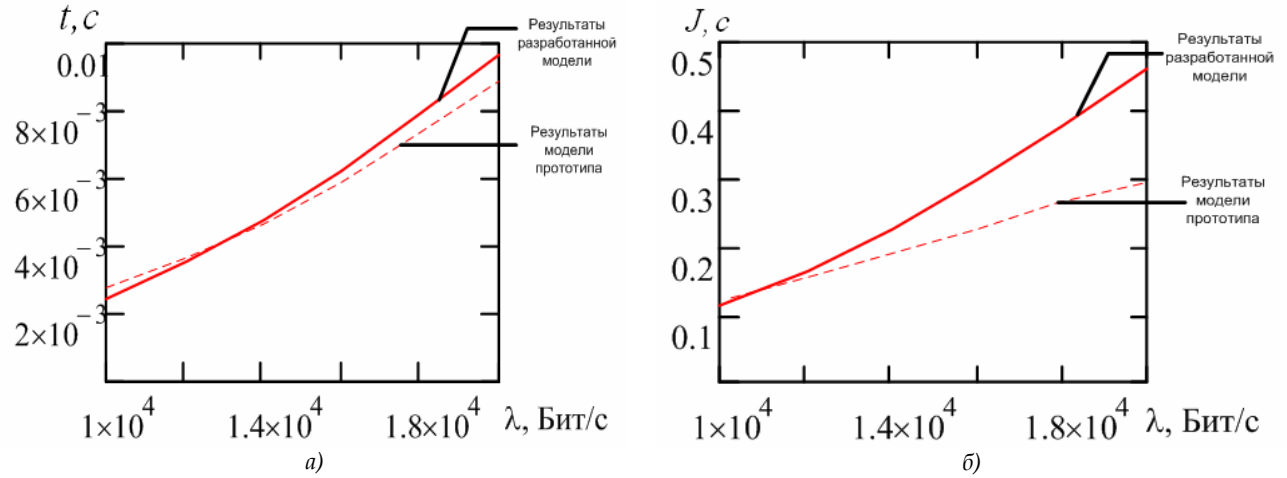
Появление в компьютерных сетях новых видов данных, таких как *IP*-телефония, потоковое аудио и видео и другие мультимедийные приложения, файлы обмена с облачными ресурсами обусловило появление новых требований, связанных с обеспечением минимальных задержек информационных пакетов (кадров) и их джиттера. В качестве основных критериев классификации потока данных в компьютерных сетях выбраны три его характеристики: относительная предсказуемость скорости передачи данных, чувствительность к задержкам пакетов, чувствительность данных к потерям и искажениям пакетов.

Сравнительные исследования результатов *GERT*-моделирования технологии передачи и обработки метаданных

Проведем сравнительные исследования разработанной математической модели технологии облачной антивирусной защиты ТКС. Для такого исследования и соответственно оценки в качестве эталонной выберем математическую модель технологии передачи данных в процессе информационного обмена специализированными сигнатурами с облачными антивирусными системами на основе *GERT*-сети, представленную в работах [3, 8-12].

В качестве исходных параметров моделирования и сравнительной оценки были выбраны числовые значения характеристик процесса передачи хеш-файла метаданных, а также обработки и доставки команд передачи управления, характерные реальному процессу функционированию ТКС с использованием средств доступа к облачным антивирусным системам: $p = 0{,}9999$; $p_i^{(k)} = 0.1\times10^{-3}, 0.2\times10^{-3},\ldots,0.4\times10^{-3}$; $\tau = 0.3\times10^{-3}$.

На рис. 5. представлены графики зависимости задержки (рис. 5 а) и джиттера (рис. 5 б) от интенсивности потока файлов метаданных, полученные в результате разработанной модели и модели – прототипа.



а) *б)*

Рис. 5. Графики зависимости задержки (а) и джиттера (б) от интенсивности потока файлов метаданных

Как видно из графиков использование разработанной *GERT*-модели технологии передачи файлов метаданных, а также обработки и доставки команд передачи управления и учет в ней возможности разбиения файла метаданных и команд передачи управления на кадры позволит до

1,2 раз повысить точность при оценке временной характеристики, и до 1,4 раз при оценке джиттера времени передачи и обработки файлов метаданных и команд передачи управления.

Таким образом, результаты оценки точности результатов моделирования подтверждают факт целесообразности использования разработанной *GERT*-модели технологии передачи хеш-файла метаданных и команд передачи управления при проектировании систем антивирусной защиты современных ТКС.

Выводы

В статье разработан комплекс математических *GERT*-моделей технологии облачной антивирусной защиты ТКС. Их отличительной особенностью является учет необходимости обработки метаданных и формирования команд передачи управления в облачных антивирусных системах.

В ходе решения поставленной задачи на первом этапе разработана математическая модель и проведено исследование вероятностно-временных характеристик алгоритмов и программ формирования и обработки метаданных в облачных антивирусных системах. Ее отличительной особенностью является учет необходимости формирования команд передачи управления программному клиенту ТКС. Это позволило повысить точность результатов оценки временных характеристик до 1,7 раз, и характеристик джиттера до 4,5 раз.

На втором этапе моделирования разработаны *GERT*-модели ТКС формирования и обработки метаданных в облачных антивирусных системах, отличающиеся от известных учетом многосвязности ТКС и возможности разбиения файла метаданных и команд передачи управления на кадры. Использование разработанных *GERT*-моделей позволит до 1,2 раз повысить точность при оценке временной характеристики, и до 1,4 раз при оценке джиттера времени передачи и обработки файлов метаданных и команд передачи управления.

Література

[1] Бабанин Д.В. Оценка структурной защищенности компьютерной сети от вирусных атак / Д.В. Бабанин // Математическое и программное обеспечение вычислительных систем: межвуз. сб. науч. тр. / Под ред. А.Н. Пылькина – Рязань: РГРТУ, 2011. – С. 133-138.

[2] Касперский К. Техника сетевых атак. [Електронний ресурс]. – Режим доступу до ресурсу: http://rghost.ru/download/43730077/8e48b6263ce45c7dc2a65a7453383dc33b22486d/Крис%20Касперски%20-%20Техника%20сетевых%20 атак.pdf.

[3] Семенов С.Г. Защита данных в компьютеризированных управляющих системах / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – LAP Lambert Academic Publishing GmbH & Co. KG (Саарбрюккен, Германия), 2014. – 236 с.

[4] Cloud security, Deep Dive series, August 2011 [Электронный ресурс]. – Режим доступа к ресурсу: http://www.slideshare.net/kimrenejensen/cloud-security-deep-dive-2011#14375029197881&fbinitialized.

[5] ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология Методы и средства обеспечения безопасности Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Електронний ресурс]. – Режим доступу до ресурсу: http://www.rfcmd.ru/sphider/docs/InfoSec/GOST-R_ISO_IEC_13335-1-2006.htm.

[6] ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции [Електронний ресурс]. – Режим доступу до ресурсу: http://protect.gost.ru/document.aspx?control=7&id=179072.

[7] Кингман Дж. Пуассоновские процессы / Дж. Кингман М.:МЦНМО, 2007. – 136 с.

[8] Смирнов А.А. Разработка математической GERT-модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / А.А. Смирнов, Мохамад Абу Таам Гани // Информационные системы в управлении, образовании, промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – 498 с.

[9] Смирнов А.А. Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Абу Таам Гани // Збірник наукових праць «Системи обробки інформації». – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.

[10] Смирнов С.А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Збірник наукових праць «Системи обробки інформації». – Випуск 9(125). – Х.: ХУПС – 2014. – С. 105-110.

[11] Смирнов С.А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – Вип. 3(43) – Х.: ХУПС – 2015. – С. 92-100.

[12] Смирнов С.А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Вип. 3(19). – Х.: ХУПС. – 2015. – С. 123-126.

УДК 004.49.5 (045)

Смірнов А.А., Дідик А.К., Дреєв А.М., Смірнов С.А. Комплекс GERT-моделей технології хмарного антивірусного захисту телекомунікаційної системи

Анотація. *У даній статті розроблено комплекс математичних GERT-моделей технології хмарного антивірусного захисту телекомунікаційної системи (ТКС), що дозволило отримати аналітичні вирази для розрахунку часу передачі файлів метаданих і формування та доставки команд передачі управління. Розроблено математичну модель і проведено дослідження ймовірнісно-часових характеристик алгоритмів і програм формування та обробки метаданих в хмарних антивірусних системах. Її відмінною рисою є облік необхідності формування команд передачі управління програмному клієнту ТКС. На другому етапі моделювання розроблені GERT-моделі технології формування та обробки метаданих в хмарних антивірусних системах. Особливістю даних моделей є врахування низки технологічних особливостей ТКС (гетерогенність, багатозв'язковість, можливість розбиття файлу метаданих і команд передачі управління на кадри та ін.).*

Ключові слова: *захист інформації, хмарні антивіруси, телекомунікаційні мережі, GERT-модель.*

Smirnov O., Didyk O., Dreyev O., Smirnov S. GERT model complex for cloud antivirus security of telecommunication system

Abstract. *In this paper, was developed a complex of mathematical models of GERT cloud antivirus technologies telecommunication system, which made it possible to obtain analytical expressions for the calculation of time transferring files and metadata creation and delivery of transfer of control commands. A mathematical model and a study probability-time characteristics of algorithms and programs of formation and processing of metadata in the cloud antivirus system. Its distinctive feature is the account of the need to form teams of transmission control software for telecommunication system client. In the second stage simulation model developed by GERT technology formation and processing of metadata in the cloud antivirus system. A special feature of these models is the consideration of a number of technological features of telecommunication system (heterogeneity, a multiply, the ability to partition the file metadata and control-transfer instructions to staff and others.).*

Key words: *information security, cloud antivirus software, telecommunication networks, GERT model.*

Отримано *12 жовтня 2015 року*, затверджено редколегією *30 жовтня 2015 року*